Abstract of the Invention

A method for improving an established Authentication and Key Agreement procedure which prevents rogue mobiles from fraudulently gaining access to a communication system. The communication system periodically broadcasts a challenge interrogation message requesting that a mobile, which is currently validated to use the system, to authenticate itself to the system. The mobile computes an authentication response based on information known only to the communication system and the USIM of the mobile and transmits said response to the communication system. The communication system also computes an authentication response and compares said response with that received from the mobile. A mobile is authenticated by the communication system when the two authentication responses are equal. Otherwise, the mobile is not given access to the communication system.